(19) JAPANESE PATENT OFFICE

PATENT ABSTRACTS OF JAPAN

(11) Publication number: **10027206 A**

(43) Date of publication of application: **27.01.98**

(51) Int. Cl **G06F 19/00**
G06F 17/60
G06K 17/00
G07D 9/00
G07F 7/08

(21) Application number: **08180394**

(22) Date of filing: **10.07.96**

(71) Applicant: **HITACHI LTD HITACHI VIDEO IND INF SYST INC**

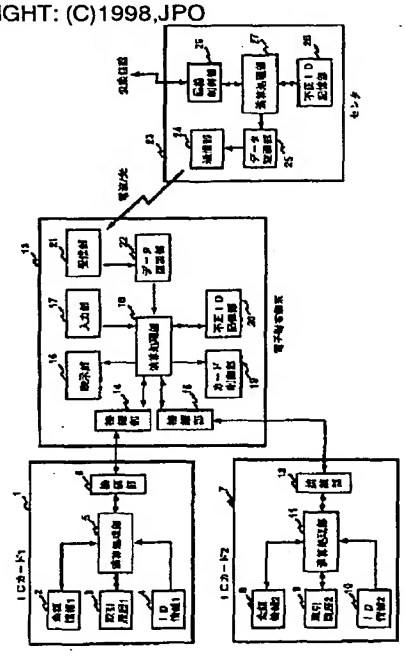
(72) Inventor: **MATSUMOTO KENJI**
ITO SHIGEYUKI
TAKAMI MINORU
INOUE MASAYUKI

(54) **ELECTRONIC PURSE ILLEGAL USE PREVENTING SYSTEM**

(57) Abstract:

PROBLEM TO BE SOLVED: To prevent the illegal use of an IC card even in an off-line processing for not performing circuit inquiry in a bank and a center by transmitting the ID number information of the IC card which is stolen or the like from the center and receiving an illegal ID number and checking the IC card on the side of an electronic purse terminal equipment.

SOLUTION: When an owner of the IC card inserts two sheets of the IC cards to the electronic purse terminal equipment 13 and depresses a remittance button in an input part 17, ID information 1 and the ID information 2 stored inside the IC card 1 and the IC card 2 are read out and supplied through connection parts 6, 12, 14 and 15 to an arithmetic processing part 18. In the arithmetic processing part 18, illegal ID number information registered in an illegal ID number storage part 20 inside the electronic purse terminal equipment 13 is read, whether or not the ID information 1 and the ID information 2 are registered as the illegal ID number information is checked, and when it is discriminated that it is the illegally used IC card, the IC card is changed to a state incapable of taking out electronic money and forcedly ejected.



(19)日本国特許庁（ＪＰ）　(12)**公開特許公報（Ａ）**　(11)特許出願公開番号

特開平10－27206

(43)公開日　平成10年(1998)１月27日

(51)Int.Cl.[6]		識別記号	庁内整理番号	ＦＩ		技術表示箇所
Ｇ０６Ｆ	19/00			Ｇ０６Ｆ 15/30	３３０	
	17/60			Ｇ０６Ｋ 17/00	Ｌ	
Ｇ０６Ｋ	17/00			Ｇ０７Ｄ 9/00	４６１Ｚ	
Ｇ０７Ｄ	9/00	４６１		Ｇ０６Ｆ 15/21	３４０Ｃ	
Ｇ０７Ｆ	7/08			15/30	３５０	

審査請求　未請求　請求項の数13　ＯＬ　（全 14 頁）　最終頁に続く

(21)出願番号　特願平8－180394

(22)出願日　平成８年(1996)７月10日

(71)出願人　000005108
株式会社日立製作所
東京都千代田区神田駿河台四丁目６番地

(71)出願人　000233136
株式会社日立画像情報システム
神奈川県横浜市戸塚区吉田町292番地

(72)発明者　松本　健司
神奈川県横浜市戸塚区吉田町292番地株式会社日立製作所マルチメディアシステム開発本部内

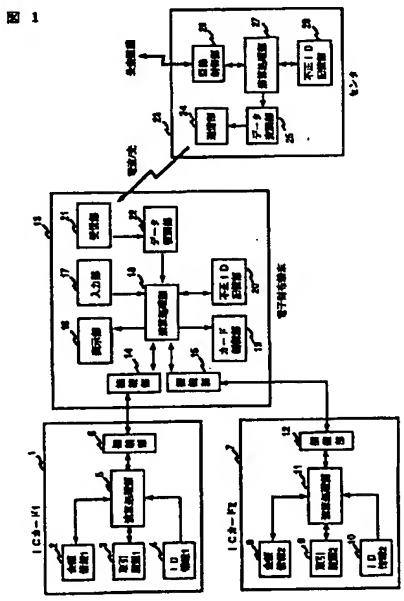
(74)代理人　弁理士　小川　勝男

最終頁に続く

(54)【発明の名称】　電子財布不正防止システム

(57)【要約】
【課題】電子財布システムでは、銀行や管理センタを経由しないオフライン処理であるため、盗難に遭ったＩＣカードの不正使用を防止するのが困難である。
【解決手段】センタから盗難に遭ったＩＣカード１のＩＤ番号情報を電波や光を用いて無線で伝送し、端末装置でこの不正ＩＤ番号の受信とＩＣカード１のチェックを行う。

図１



1

【特許請求の範囲】

【請求項１】電子マネー情報とＩＤ情報を格納するＩＣカードと、上記ＩＣカードの情報を読み取り，書き込みを行うＩＣカード読み書き手段と、上記ＩＣカードの装着及び排出を制御するＩＣカード制御手段と、不正ＩＤ情報を受信する受信手段と、上記不正ＩＤ情報を記録する記録手段と、上記ＩＤ情報と上記不正ＩＤ情報とを比較する演算処理手段とを有する電子財布端末装置とから構成され、上記演算処理手段の出力により、上記ＩＤ情報が上記不正ＩＤ情報として記録されている場合は、上記ＩＣカードでの商取引を行わないことを特徴とする電子財布不正防止システム。

【請求項２】請求項１において、上記不正ＩＤ情報は電波や光を用いて伝送される電子財布不正防止システム。

【請求項３】電子マネー情報とＩＤ情報を格納するＩＣカードと、上記ＩＣカードの情報を読み取り，書き込みを行うＩＣカード読み書き手段と、上記ＩＣカードの装着及び排出を制御するＩＣカード制御手段と、不正ＩＤ情報を受信する受信手段と、上記不正ＩＤ情報を記録する記録手段と、上記ＩＤ情報と上記不正ＩＤ情報とを比較する演算処理手段とを有する電子財布端末装置とから構成され、上記演算処理手段の出力により、上記ＩＤ情報が上記不正ＩＤ情報として記録されている場合は、上記ＩＣカードでの商取引を行わないことを特徴とする電子財布不正防止システム。

【請求項４】請求項３において、上記不正ＩＤ情報は公衆回線網を通して伝送される電子財布不正防止システム。

【請求項５】電子マネー情報とＩＤ情報を格納するＩＣカードと、上記ＩＣカードの情報を読み取り，書き込みを行うＩＣカード読み書き手段と、上記ＩＣカードの装着及び排出を制御するＩＣカード制御手段と、変調された不正ＩＤ情報を受信する受信手段と、上記不正ＩＤ情報を復調する復調手段と、上記復調された不正ＩＤ情報を記録する記録手段と、上記ＩＤ情報と上記不正ＩＤ情報とを比較する演算処理手段とを有する電子財布端末装置とから構成され、上記演算処理手段の出力により、上記ＩＤ情報が上記不正ＩＤ情報として記録されている場合は、上記ＩＣカードでの商取引を行わないことを特徴とする電子財布不正防止システム。

【請求項６】請求項５において、上記不正ＩＤ情報は電波や光を用いて伝送される電子財布不正防止システム。

【請求項７】電子マネー情報とＩＤ情報を格納するＩＣカードと、上記ＩＣカードの情報を読み取り，書き込みを行うＩＣカード読み書き手段と、上記ＩＣカードの装着及び排出を制御するＩＣカード制御手段と、変調された不正ＩＤ情報を受信する受信手段と、上記不正ＩＤ情報を復調する復調手段と、上記復調された不正ＩＤ情報を記録する記録手段と、上記ＩＤ情報と上記不正ＩＤ情報とを比較する演算処理手段とを有する電子財布端末装置とから構成され、上記演算処理手段の出力により、上記ＩＤ情報が上記不正ＩＤ情報として記録されている場合は、上記ＩＣカードでの商取引を行わないことを特徴とする電子財布不正防止システム。

2

【請求項８】請求項７において、上記不正ＩＤ情報は公衆回線網を通して伝送される電子財布不正防止システム。

【請求項９】電子マネー情報を記録する手段と、ＩＤ情報を記録する手段と、信用情報を記録する手段と、上記信用情報の有効期限を判断する演算処理手段とを有するＩＣカードと、上記ＩＣカードの情報を読み取り，書き込みを行うＩＣカード読み書き手段と、上記ＩＣカードの装着及び排出を制御するＩＣカード制御手段とを有する電子財布端末装置とから構成され、上記演算処理手段の出力により、上記信用情報が有効期限内の場合のみ、上記ＩＣカードでの商取引を行うことを特徴とする電子財布不正防止システム。

【請求項１０】電子マネー情報を記録する手段と、ＩＤ情報を記録する手段と、信用情報を記録する手段と、上記信用情報の有効期限を判断する演算処理手段とを有するＩＣカードと、上記ＩＣカードの情報を読み取り，書き込みを行うＩＣカード読み書き手段と、上記ＩＣカードの装着及び排出を制御するＩＣカード制御手段と、上記信用情報を送受信する送受信手段とを有する電子財布端末装置とから構成され、上記演算処理手段の出力により、上記信用情報が有効期限内の場合のみ、上記ＩＣカードでの商取引を行うことを特徴とする電子財布不正防止システム。

【請求項１１】請求項１０において、上記信用情報は電波や光を用いて伝送される電子財布不正防止システム。

【請求項１２】電子マネー情報を記録する手段と、ＩＤ情報を記録する手段と、信用情報を記録する手段と、上記信用情報の有効期限を判断する演算処理手段とを有するＩＣカードと、上記ＩＣカードの情報を読み取り，書き込みを行うＩＣカード読み書き手段と、上記ＩＣカードの装着及び排出を制御するＩＣカード制御手段と、上記信用情報を送受信する送受信手段とを有する電子財布端末装置とから構成され、上記演算処理手段の出力により、上記信用情報が有効期限内の場合のみ、上記ＩＣカードでの商取引を行うことを特徴とする電子財布不正防止システム。

【請求項１３】請求項１２において、上記不正ＩＤ情報は公衆回線網を用いて伝送される電子財布不正防止システム。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】本発明は、電子財布システムを用いて商取引を行う際に、盗難等に遭ったＩＣカードのＩＤ番号情報を電波や光を用いて無線で流し、かつ、取引端末装置側でこの不正ＩＤ番号の受信及びチェック

を行うことにより、銀行等を経由しないオフライン処理においてもＩＣカードの不正使用を防止することを可能とした電子財布不正防止システムに関する。

【０００２】

【従来の技術】現在、商取引の際には、現金の代わりにクレジットカードによる支払いが普及しているが、支払いが後払い処理となるため、基本的には商取引の際に信用照会が必要となる。そのため、小売店側では銀行やセンタと公衆回線でつなぎ、オンライン処理で信用照会を行う。また、販売後も伝票処理等の手間や経費がかかるため、クレジットカードによる支払いは少額の買い物には向かない。

【０００３】一方、クレジットカードによる支払いとは別に、特開平３－９２９６６号公報に記載されているように、ＩＣカードを使用した電子財布システムによる商取引の完全なキャッシュレス化も検討されている。これは、ＩＣカード内のメモリに任意に指定された金額情報を書き込み、精算時にはＩＣカードから必要な金額情報を送信することで、現金を用いずに商取引を完了させるシステムである。

【０００４】

【発明が解決しようとする課題】この電子財布システムによる商取引が実現した場合、ＩＣカード内の金額情報をやり取りするだけで支払いが終了するため、即時決済となり、小売店側では銀行やセンタへの信用照会及び伝票処理等が不要となる。このようなオフライン処理による支払いでは、クレジットカードのようなオンライン処理と比べて経費がかからないため、少額の買い物でも対応可能となる。

【０００５】一方、電子財布システムでは、商取引時に銀行やセンタ等での信用照会がなされないため、ＩＣカードが盗難に遭った場合や紛失した場合に不正使用を防止することが困難となる。そのため、ＩＣカード自体に暗証番号で鍵をかけることにより、所有者以外は金額情報を取り出せなくすることも可能だが、鍵をかけ忘れた場合は不正使用を防止することは不可能であり、何らかの対策が必要である。

【０００６】

【課題を解決するための手段】上記目的を達成するために、本発明では、電子マネー情報とＩＤ情報を格納するＩＣカードと、上記ＩＣカードの情報読み取り，書き込みを行うＩＣカード読み書き手段と、上記ＩＣカードの装着及び排出を制御するＩＣカード制御手段と、変調された不正ＩＤ情報を受信する受信手段と、上記不正ＩＤ情報を復調する復調手段と、上記復調された不正ＩＤ情報を記録する記録手段と、上記ＩＤ情報と上記不正ＩＤ情報とを比較する演算処理手段とを有する電子財布端末装置とで構成する。

【０００７】そして、上記演算処理手段の出力により、上記ＩＤ情報が上記不正ＩＤ情報として記録されている場合は、上記ＩＣカードでの商取引を行わないように制御を行う。

【０００８】なお、上記不正ＩＤ情報は電波や光を用いてセンタから無線で伝送する場合や公衆回線網を通して伝送する場合が考えられる。

【０００９】以上のように、本発明ではセンタから盗難等に遭ったＩＣカードのＩＤ番号情報を送信し、かつ、電子財布端末装置側でこの不正ＩＤ番号の受信とＩＣカードのチェックを行うことにより、銀行やセンタで信用照会を行わないオフライン処理においてもＩＣカードの不正使用を防止することが可能となる。

【００１０】

【発明の実施の形態】本発明の実施例を図１ないし図８を用いて説明する。

【００１１】図１は本発明を用いた電子財布端末装置の一実施例であり、センタから盗難等に遭ったＩＣカードのＩＤ番号情報が電波や光（例えば、赤外光など）を用いて無線で伝送され、電子財布端末装置側でこの不正ＩＤ番号のチェックを行う。

【００１２】１はＩＣカード１、２は金額情報記憶部１、３は取引履歴情報記憶部１、４はＩＤ情報記憶部１、５は演算処理部、６は接続部、７はＩＣカード２、８は金額情報記憶部２、９は取引履歴情報記憶部２、１０はＩＤ情報記憶部２、１１は演算処理部、１２は接続部、１３は電子財布端末装置、１４，１５は接続部、１６は表示部、１７は入力部、１８は演算処理部、１９はカード制御部、２０は不正ＩＤ情報記憶部、２１は受信部、２２はデータ復調部、２３はセンタ、２４は送信部、２５はデータ変調部、２６は回線制御部、２７は演算処理部、２８は不正ＩＤ記憶部である。

【００１３】まず始めに、不正ＩＤ番号情報を送信するセンタ側の詳細を説明する。ＩＣカードの所有者は、自分のＩＣカードが盗難に遭った場合や紛失した場合に公衆回線を通してその旨をセンタに伝えるが、この情報は、回線制御部２６を通して演算処理部２７に供給される。演算処理部２７では、このＩＣカードのＩＤ番号を検索し、不正ＩＤ番号情報として不正ＩＤ番号情報記憶部２８に登録する。その後、不正ＩＤ番号情報記憶部に登録されたその他の不正ＩＤ番号と共にデータ変調部２５に変調され、送信部２４から電波や赤外光などの光を用いて無線で伝送される。

【００１４】次に、電子財布端末装置側の詳細を説明する。電子財布端末装置１３には、電波や光で送信されたデータの受信部２１があるが、受信された不正ＩＤ番号情報はデータ復調部２２で復調後に演算処理部１８に供給され、その後、不正ＩＤ番号情報記憶部２０に登録される。この、不正ＩＤ番号情報の登録は、電子財布端末装置の電源が入れられた状態の時に自動的に行われるが、所有者がボタンを押すと登録されるような手動にしてもよい。

【００１５】ここでは、図２を用いて、電子マネーにより個人間決済を行う場合を例に処理の流れを説明する。ＩＣカード所有者が２枚のＩＣカードを電子財布端末装置１３に挿入して（Ｓ１０１）、入力部１７で送金ボタンを押すと（Ｓ１０２）、ＩＣカード１内に記憶されたＩＤ情報１が読み取られて、接続部６，１４を通して演算処理部１８に供給される（Ｓ１０３）。同様に、ＩＣカード２内に記憶されたＩＤ情報２も接続部１２，１５を通して演算処理部１８に供給される（Ｓ１０４）。その後、電子財布端末装置内の不正ＩＤ番号記憶部２０に登録された不正ＩＤ番号情報が読み取られて、演算処理部１８に供給される（Ｓ１０５）。

【００１６】演算処理部１８では、ＩＤ情報１及びＩＤ情報２が不正ＩＤ番号情報として登録されているかどうかのチェックを行い（Ｓ１０６）、不正に使用されているＩＣカードであることが判明すると、そのＩＣカードから電子マネーが取り出せない状態（以下、これをＬｏｃｋ　Ｏｕｔ状態と呼ぶ）にＩＣカードを変更して（Ｓ１０８）、カード制御部１９により強制的にＩＣカードを排出する（Ｓ１１０）。そのため、ＩＣカードが盗難等に遭った際にカード所有者がセンタに申し出ることにより、そのＩＣカードの不正使用は防止される。

【００１７】一方、正常なＩＣカードである場合は、演算処理部５，１１で送金処理がなされて（Ｓ１０７）、金額情報記憶部１，２内の電子マネー残高が更新される。また、取引履歴情報記憶部１，２も同様に更新されて、取引履歴が記録される。ここで、送金処理を終了すると（Ｓ１０９）、ＩＣカードが排出される（Ｓ１１０）。なお、表示部１６には、決済する金額情報や処理の内容が表示される。

【００１８】実施例では、電子財布端末装置を用いて電子マネーの決済を行う際にＩＤ番号のチェックを行うが、図３に示すようにＩＣカードを電子財布端末に挿入するとすぐにＩＤ番号のチェックを行うようにしてもよい。この場合、不正なＩＤ番号であるとカードはすぐにＬｏｃｋ　Ｏｕｔ状態になるが（Ｓ２０６）、正常なＩＣカードの場合はＩＣカードの残高照会や取引履歴の確認等の操作を行うことが可能となる（Ｓ２０５）。

【００１９】以上のように、不正なＩＤ番号情報を電波や光を用いて無線で伝送することにより、電子財布端末装置を用いて決済を行うようなオフライン処理においてもＩＣカードの不正使用を防止することが可能となる。この場合、不正ＩＤ番号情報の伝送方法としては、例えば専用のＡＭ放送やＦＭ文字多重放送などがあげられる。また、携帯電話と電子財布端末を組み合わせた装置では、無線による公衆回線で伝送することも可能である。

【００２０】次に、図４を用いて本発明を用いたＰＯＳ端末の一実施例を説明する。ＰＯＳ端末等の場合、公衆回線を用いて売上金を銀行や本部に送金するため、不正

ＩＤ番号情報も公衆回線を用いて伝送することが可能となる。３０はＰＯＳ端末、３１は回線制御部、３２は売上金額情報記憶部、３３は売上履歴情報記憶部、３４はセンタである。

【００２１】この場合も、ＩＣカードの盗難届けは公衆回線を通してセンタに送られるが、センタでは不正ＩＤ番号情報記憶部２８に登録されたデータを回線制御部２６を通して公衆回線で各ＰＯＳ端末に伝送する。また、伝送されたデータは、回線制御部３１を介して各ＰＯＳ端末の不正ＩＤ番号情報記憶部２０に登録される。

【００２２】ここでは、図５を用いて処理の流れを説明する。ＩＣカードの所有者がカードにより支払いを行う場合は、まず、ＩＣカードをＰＯＳ端末３０に挿入し（Ｓ３０１）、その後、買い物金額が表示部１６に表示される（Ｓ３０２）。ＩＣカードで支払いを行う場合は（３０３）、ＩＣカード内のＩＤ情報が読み取られて（Ｓ３０４）、接続部６，１４を介して演算処理部１８に供給される。その後、ＰＯＳ端末内の不正ＩＤ番号情報が読み取られて（Ｓ３０５）、同様に演算処理部１８に供給される。

【００２３】演算処理部１８では、ＩＤ情報が不正番号情報として登録されているかどうかのチェックを行い（Ｓ３０６）、不正に使用されているＩＣカードであることが判明すると、そのＩＣカードをＬｏｃｋ　Ｏｕｔ状態に変更して（Ｓ３０８）、カード制御部１９により強制的にＩＣカードを排出する（Ｓ３１３）。

【００２４】一方、正常なＩＣカードである場合は、次に、ＩＣカード内の金額情報が読み取られて（Ｓ３０７）、買い物金額の支払いが可能かどうかのチェックがなされる（Ｓ３０９）。残高が足りない場合はその旨が表示部１６に表示される（Ｓ３１１）と共に、ＩＣカードが排出されて（Ｓ３１３）、取引が終了する。一方、支払いが可能な場合は、演算処理部５，１８で送金処理がなされて、ＩＣカード内の金額情報記憶部２が更新される（Ｓ３１０）と共に、取引履歴情報記憶部３も更新されて取引履歴が記録される。また、ＰＯＳ端末内の売上金額情報記憶部３２が更新され（Ｓ３１２）、さらに、売上履歴情報記憶部３３も更新された後に、ＩＣカードが排出される（Ｓ３１３）。

【００２５】以上により、公衆回線で伝送された不正ＩＤ番号情報がＰＯＳ端末でチェックされるため、ＩＣカードの不正使用を防止することができる。

【００２６】次に、図６を用いて、不正ＩＤ番号データの変調部及び復調部を説明する。不正ＩＤ番号情報を無線で伝送する場合、データの偽造を防ぐために何らかの暗号化が必要となる。そこで、本発明では、図６に示すように暗号鍵により不正ＩＤ番号情報の暗号化を行う一例を説明する。

【００２７】まず、データ変調部２５では、演算処理部から供給された不正ＩＤ番号情報をＩＤ暗号化部４５で

暗号化する。この場合、ＩＤ暗号化部鍵情報記憶部４８に格納されたＩＤ暗号化部鍵により、あらかじめ定められた規則で暗号化を行う。また、このＩＤ暗号化部鍵はＩＤ暗号化部鍵情報の暗号化部４７で暗号化されるが、この場合も暗号化の際には暗号鍵記憶部４６に格納された暗号鍵により、一定の規則で暗号化される。これらの暗号化されたデータは、送信部２４から電波や光などの無線で送信される。

【００２８】一方、無線で送信されたデータは受信部２１で受信されて、データ復調部２２に供給される。暗号化されたデータの中で、ＩＤ暗号化部鍵は復号化部５０で復号化されるが、復号化部５０での処理の際には暗号鍵記憶部５１に格納された暗号鍵により定められた規則で復号化される。なお、この暗号鍵はセンタにより一括管理されている。そのため、センタから送信された正式なデータを受信した場合のみ、復号化部５０でＩＤ暗号化部鍵を復号化することができる。その後、このＩＤ暗号化部鍵により、不正ＩＤ番号情報がＩＤ復号化部４９で復号化される。

【００２９】以上により、センタから送られてきた正式な不正ＩＤ番号情報のみが再生されるので、データの偽造を防ぐことが可能となる。

【００３０】次に、ＩＣカード自体に信用情報を登録する例を説明する。実施例では、センタから送られてくる不正ＩＤ番号情報を端末側でチェックすることでＩＣカードの不正使用を防止したが、ＩＣカード自体に信用情報を定期的に登録することにより不正防止を行うことも可能である。図７では、ＩＣカード３５がＰＯＳ端末３６に挿入されるとＩＣカードのＩＤ情報が読み取られて、ＰＯＳ端末の回線制御部３１を介してセンタ３４に公衆回線で送られる。センタではこのＩＤ番号が不正ＩＤ番号記憶部２８に登録されていないかどうかのチェックを行い、不正なものではないことを確認すると信用情報が公衆回線を通ってＰＯＳ端末３６に送信され、その後、この信用情報がＩＣカード３５内の信用情報記憶部３７に格納される。ここで、不正なＩＤ番号の場合は、信用情報記憶部３７内のデータは更新されない。

【００３１】ＩＣカードを用いて商取引を行う場合、決済時にＩＣカードに登録された信用情報のチェックを演算処理部５で行い、信用情報が正しく登録されていないカードでは決済が行えないようにすることで不正使用を防止することができる。この場合、信用情報には期限を設けて、かつ、ＩＣカードの所有者が定期的に信用情報の更新を行うようにすれば、不正なＩＣカードでは信用情報が更新されないため、決済を行うことができない。

【００３２】なお、この信用情報の登録は、公衆回線でセンタと接続された端末であれば可能であり、ＰＯＳ端末以外でも銀行のＡＴＭ端末等で行うこともできる。この場合、信用情報の更新は、ＰＯＳ端末やＡＴＭ端末にアクセス時に自動的に行われるが、所有者が選択すると行われるように制御してもよい。また、電波や光等の無線を用いてセンタと情報のやり取りを行ってもよい。

【００３３】ここで、図８に示すように、ＩＣカード３８内に信用情報チェック部３９を内蔵させて、信用情報を専用回路でチェックさせることも可能である。この場合、信用情報チェック部３９では、信用情報と共にＩＣカード内の取引履歴や金額情報などのデータもチェックして、ＩＣカードが真に正常なものである場合のみ取引決済を行うように制御することも可能である。また、チェック結果に基づき、信用情報記憶部３７のデータを再度更新するようにしてもよい。

【００３４】なお、信用情報チェック部はＰＯＳ端末やＡＴＭ側に持たせることも可能である。この場合、信用情報チェック部を不正に使用することも考えられるため、センタからの指令でのみ動作を行うように制御することで安全性を高めることができる。

【００３５】以上のように、ＩＣカード自体に有効期限付きの信用情報データを持たせて、所有者がオンラインで定期的に更新することにより、オフライン処理である電子財布端末を用いた場合でも不正ＩＣカードの使用を防止することができる。

【００３６】

【発明の効果】本発明では、センタから盗難等に遭ったＩＣカードのＩＤ番号情報を電波や光を用いて無線で伝送し、かつ、電子財布端末盗難等でこの不正ＩＤ番号の受信とＩＣカードのチェックを行うことにより、銀行やセンタで信用照会を行わないオフライン処理においてもＩＣカードの不正使用を防止することが可能となる。また、センタから不正ＩＤ番号を公衆回線で伝送し、ＰＯＳ端末等で不正使用のチェックを行うことも可能である。さらに、ＩＣカード自体に信用情報を持たせて、決済時にこの信用情報をチェックすることで不正防止をすることもできる。この場合、信用情報に期限を設けて、かつ、ＩＣカード所有者がオンラインで定期的に信用情報を更新することにより、不正なＩＣカードは信用情報の更新ができないため、決済を行うことができない。

【図面の簡単な説明】

【図１】本発明を用いた電子財布端末装置の一実施例のブロック図。

【図２】本発明を用いた電子財布端末装置での操作のフローチャート。

【図３】本発明を用いた電子財布端末装置での操作のフローチャート。

【図４】本発明を用いたＰＯＳ端末の一実施例のブロック図

【図５】本発明を用いたＰＯＳ端末での操作のフローチャート。

【図６】本発明を用いた不正ＩＤ番号データの変調部及び復調部の一実施例のブロック図。

【図７】本発明を用いたＰＯＳ端末の第二の実施例のブ

ロック図。

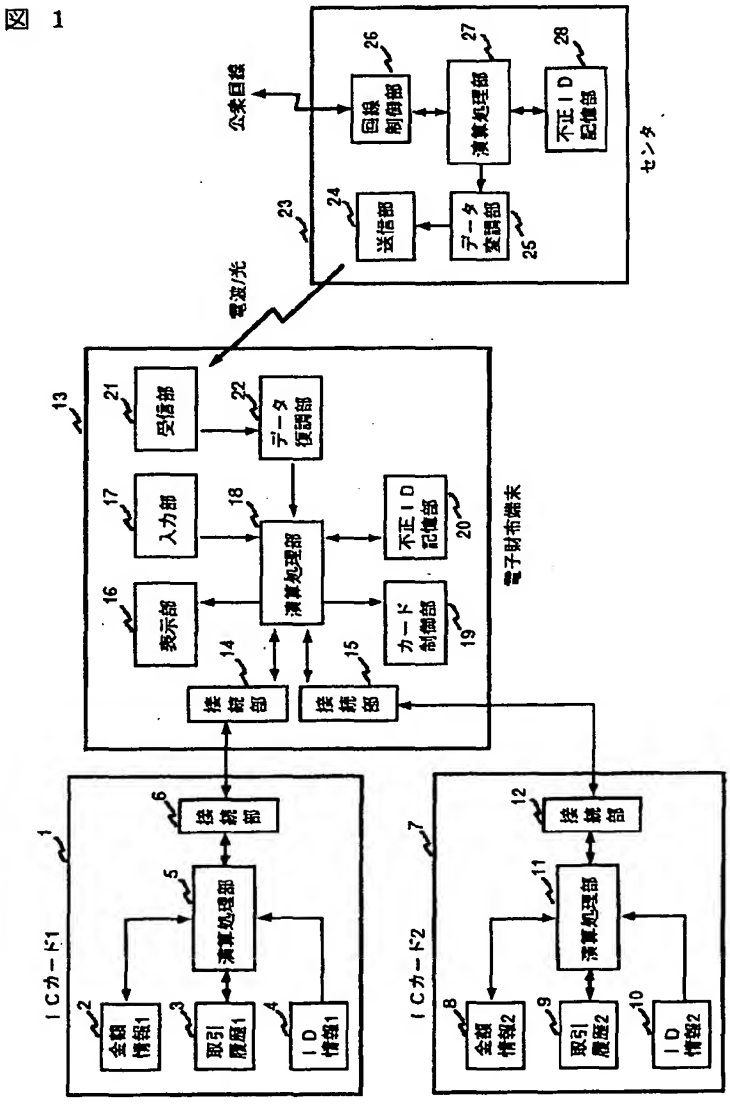
【図８】本発明を用いたＰＯＳ端末の第三の実施例のブロック図。

【符号の説明】

１…ＩＣカード、２…金額情報記憶部、３…取引履歴情報記憶部、４…ＩＤ情報記憶部、５…演算処理部、６…接続部、７…ＩＣカード、８…金額情報記憶部、９…取引履歴情報記憶部、１０…ＩＤ情報記憶部、１１…演算処理部、１２…接続部、１３…電子財布端末、１４，１５…接続部、１６…表示部、１７…入力部、１８…演算処理部、１９…カード制御部、２０…不正ＩＤ記憶部、２１…受信部、２２…データ復調部、２３…センタ、２４…送信部、２５…データ変調部、２６…回線制御部、２７…演算処理部、２８…不正ＩＤ記憶部。

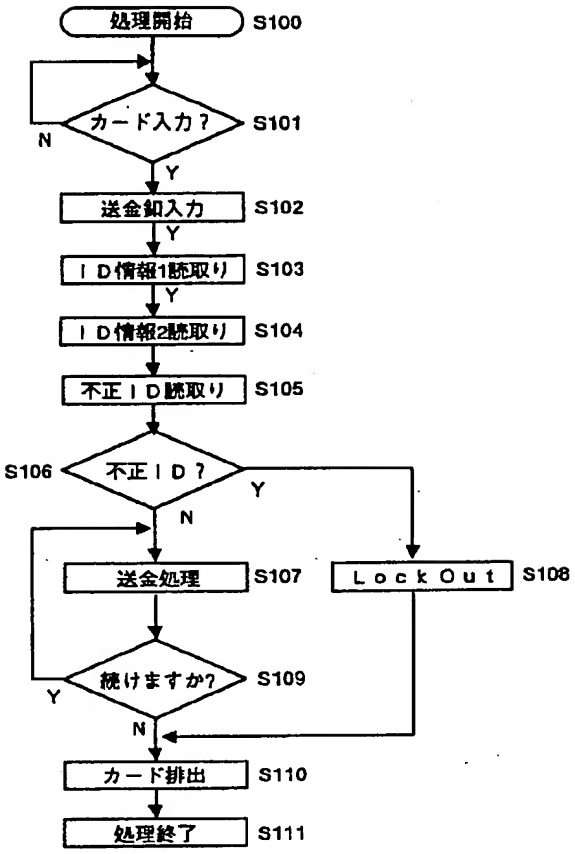
【図１】

図　1



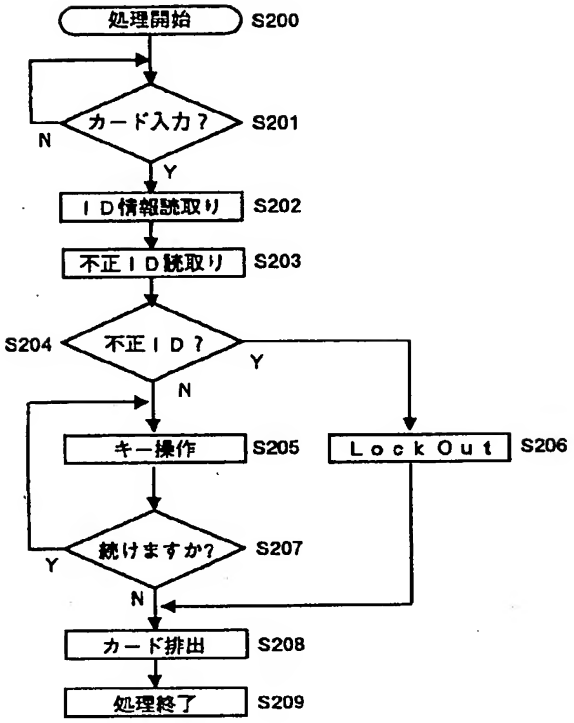
【図２】

図2


処理開始
S100
カード入力？
S101
N
Y
送金釦入力
S102
Y
ＩＤ情報1読取り
S103
Y
ＩＤ情報2読取り
S104
不正ＩＤ読取り
S105
S106
不正ＩＤ？
Y
N
送金処理
S107
Ｌｏｃｋ Ｏｕｔ
S108
続けますか?
S109
Y
N
カード排出
S110
処理終了
S111

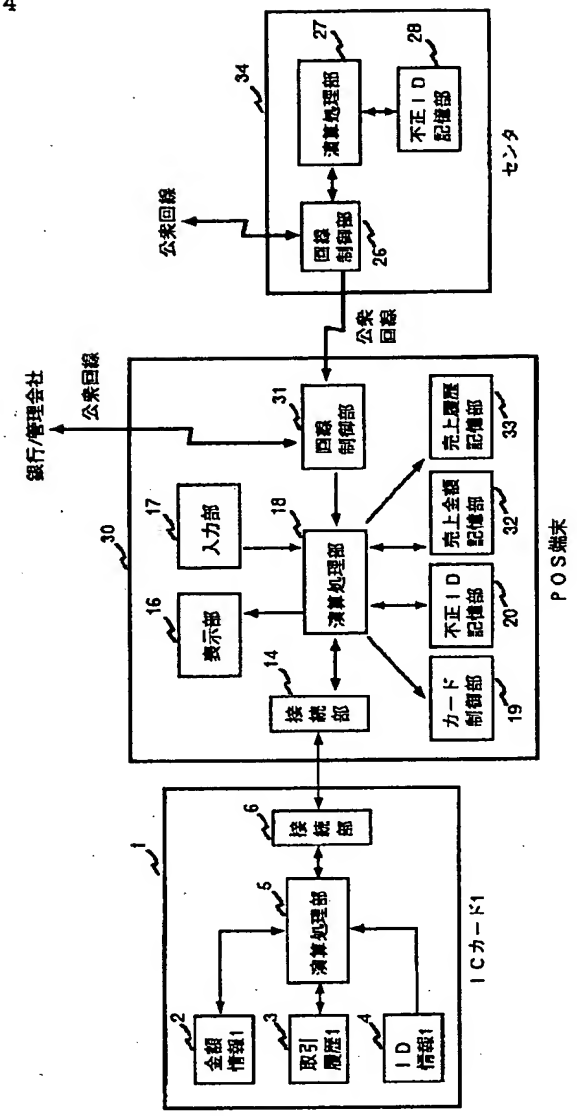
【図３】

図3


処理開始
S200
カード入力？
S201
N
Y
ＩＤ情報読取り
S202
不正ＩＤ読取り
S203
S204
不正ＩＤ？
Y
N
キー操作
S205
Ｌｏｃｋ Ｏｕｔ
S206
続けますか?
S207
Y
N
カード排出
S208
処理終了
S209

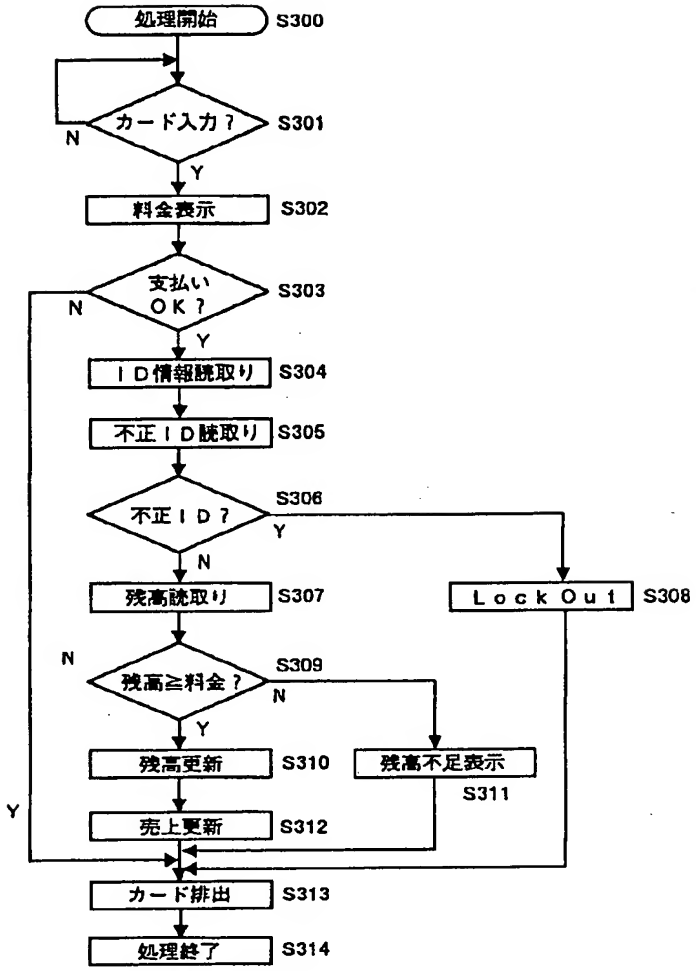
【図４】

図　４


センタ
27
演算処理部
28
不正ＩＤ記憶部
34
公衆回線
回線制御部
25
公衆回線
銀行/管理会社
公衆回線
31
回線制御部
売上履歴記憶部
33
売上金額記憶部
32
不正ＩＤ記憶部
20
カード制御部
19
POS端末
30
入力部
17
18
演算処理部
表示部
16
14
接続部
1
6
接続部
5
演算処理部
ICカード1
2
金額情報1
3
取引履歴1
4
ＩＤ情報1

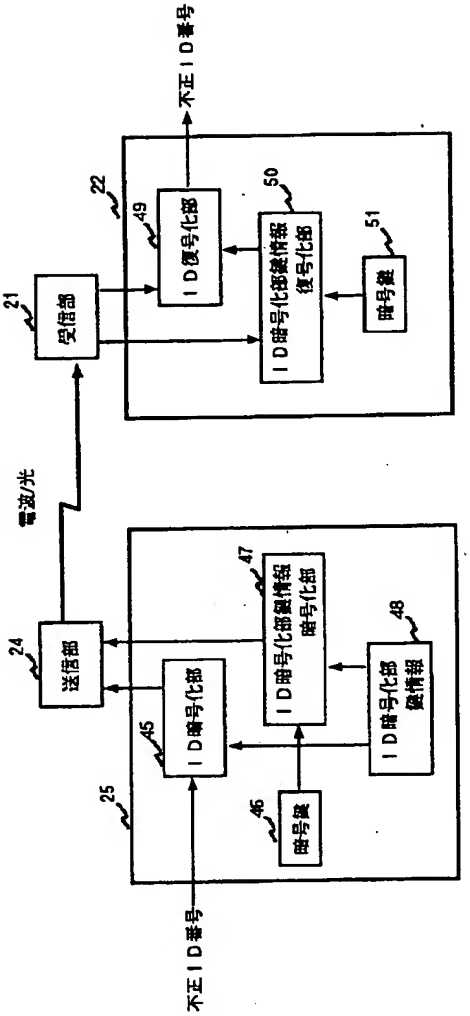
【図５】

図5


処理開始
S300
カード入力？
S301
N
Y
料金表示
S302
支払い OK？
S303
N
Y
ＩＤ情報読取り
S304
不正ＩＤ読取り
S305
不正ＩＤ？
S306
Y
N
残高読取り
S307
Ｌｏｃｋ Ｏｕｔ
S308
N
残高≧料金？
S309
N
Y
残高更新
S310
残高不足表示
S311
Y
売上更新
S312
カード排出
S313
処理終了
S314

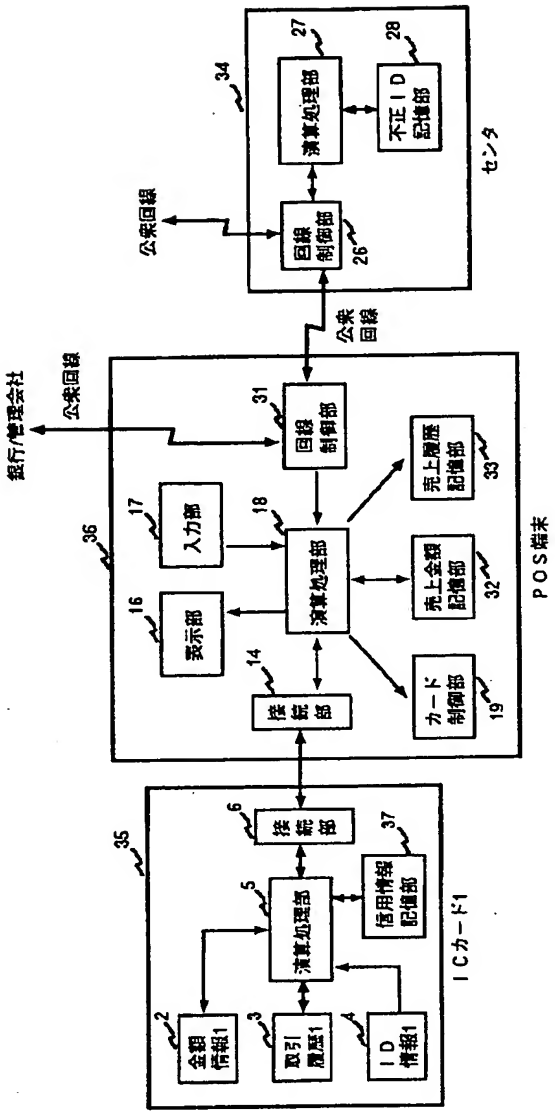
【図６】

図 6


不正ＩＤ番号
22
49
ＩＤ復号化部
50
ＩＤ暗号化部鍵情報復号化部
51
暗号鍵
21
受信部
電波/光
24
送信部
47
ＩＤ暗号化部鍵情報暗号化部
48
ＩＤ暗号化部鍵情報
45
ＩＤ暗号化部
46
暗号鍵
25
不正ＩＤ番号

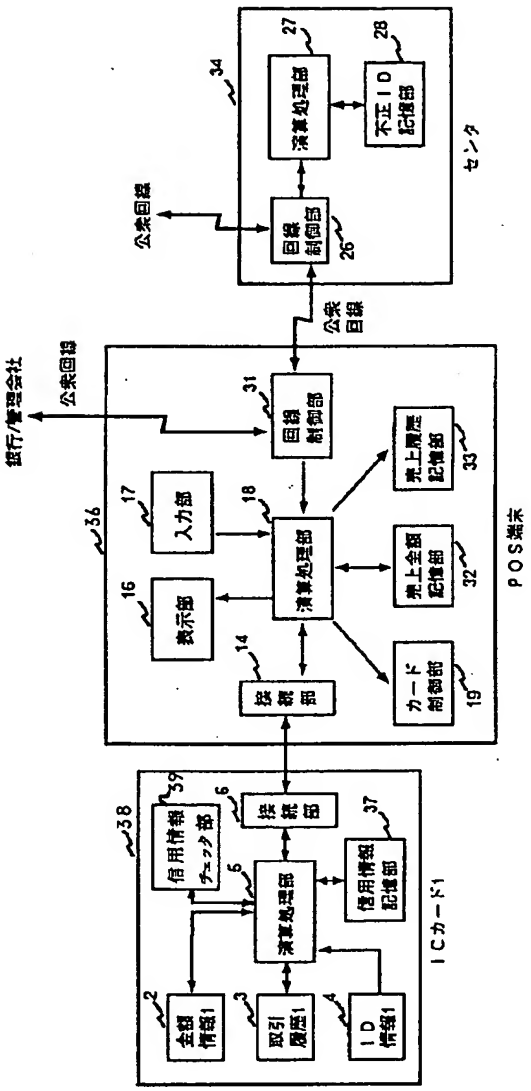
【図７】

図　7


センタ
演算処理部
27
不正ＩＤ記憶部
28
34
回線制御部
26
公衆回線
公衆回線
銀行/管理会社
公衆回線
POS端末
回線制御部
31
入力部
17
表示部
16
演算処理部
18
接続部
14
売上履歴記憶部
33
売上金額記憶部
32
カード制御部
19
36
ICカード1
接続部
6
演算処理部
5
信用情報記憶部
37
金額情報1
2
取引履歴1
3
ＩＤ情報1
4
35

【図８】

図　８



フロントページの続き

(51)Int.Cl.6	識別記号	庁内整理番号	FI	技術表示箇所
			G07F 7/08	Z

(72)発明者 伊藤 滋行
神奈川県横浜市戸塚区吉田町292番地株式会社日立製作所マルチメディアシステム開発本部内

(72)発明者 髙見 穣
神奈川県横浜市戸塚区吉田町292番地株式会社日立製作所マルチメディアシステム開発本部内

(72)発明者 井上 雅之
神奈川県横浜市戸塚区吉田町292番地株式会社日立画像情報システム内